Amendments to the Claims:

This listing of claims will replace all prior versions and listings of claims in the application.

Listing of Claims:

1. (Currently Amended) A method of processing a Session Initiation Protocol (SIP) message, the method comprising:

receiving a SIP request at a SIP node, the SIP request including a message header including data indicative of network routing locations;

determining a RECORD-ROUTE header of the SIP request;

editing the data at the SIP node;

generating a signature based upon at least a portion of the message header including the edited data;

generating a SIP node header entry; and

inserting the signature into the SIP node header entry;

wherein generating the signature includes generating the signature based upon at least a portion of the RECORD-ROUTE header of the SIP request; and

wherein inserting the signature includes inserting the signature into a RECORD-ROUTE header of the SIP node.

2. (Original) The method of claim 1, wherein the SIP node header entry is an echoed header.

3-6. (Canceled)

7. (Previously Presented) A method of processing a Session Initiation Protocol (SIP) message, the method comprising:

receiving a SIP request at a SIP node, the SIP request including a message header;

generating a signature based upon at least a portion of the message header;

generating a SIP node header entry, wherein the SIP node header entry is a VIA header;

inserting the signature into the SIP node header entry;

receiving a SIP response at the SIP node in reply to the SIP request, the SIP response comprising the VIA header for the SIP node, the VIA header including a first received signature;

verifying the first received signature;

determining a next link to a next SIP node to receive the SIP request; and

determining if the next link to the next SIP node is an untrusted link, wherein generating the first signature includes only generating the first signature if the next link is an untrusted link.

8-14. (Canceled)

15. (Previously Presented) A method of processing a Session Initiation Protocol (SIP) message, the method comprising:

receiving a SIP request at a SIP node, the SIP request including a message header;

generating a signature based upon at least a portion of the message header;

generating a SIP node header entry;

inserting the signature into the SIP node header entry;

receiving a SIP response in reply to the SIP request, the SIP response including a response header;

generating another signature based upon a RECORD-ROUTE header and a CONTACT header of the response header;

inserting the other signature into a RECORD-ROUTE header of the SIP node of the response; and

before generating the other signature, removing an existing signature from the SIP node header entry.

16-21. (Canceled)

22. (Currently Amended) The method of claim [[21]] 1, wherein inserting the ~~third~~ signature includes inserting the ~~third~~ signature as a header parameter of the RECORD-ROUTE header of the SIP node.

23. (Currently Amended) The method of claim [[21]] 1, further comprising:

receiving a SIP response at the SIP node in reply to the SIP request, the SIP response comprising the RECORD-ROUTE header for the SIP node which includes a third received signature; and

verifying the third received signature.

24. (Currently Amended) The method of claim 1 [[20]], further comprising:

determining a next link to a next SIP node to receive the SIP request; and

determining if the next link to the next SIP node is an untrusted link, wherein generating the third signature includes only generating the third signature if the next link is an untrusted link.

25. (Canceled)

26. (Currently Amended) A computer storage medium having computer executable instructions for performing steps for processing messages in a pool of servers having a first server and a second server which are constructed and arranged to be interchangeably used to process messages in the same dialog, the steps comprising:

identifying, at the first server, a public key and a private key;

receiving, at the first server, a first message including a first header;

generating a session key;

encrypting the session key with the private key;

generating, with the public key, a key signature based on the encrypted session key; ~~and~~

inserting the key signature into the first header; and

identifying a time stamp containing data representing a date and time of creation for the session key and appending the time stamp to the session key, wherein encrypting the session key includes encrypting the session key and the time stamp.

27. (Previously Presented) The computer storage medium of claim 26, further comprising:

identifying, at the second server, the public key and the private key;

receiving, at the second server, a second message including a second header, the second header comprising the key signature;

decrypting the key signature to determine the session key.

28. (Previously Presented) The computer storage medium of claim 27, further comprising:

verifying at least a portion of the second message with the session key.

29. (Previously Presented) The computer storage medium of claim 26, wherein the first message is a Session Initiation Protocol (SIP) message.

30. (Previously Presented) The computer storage medium of claim 26, wherein the first server is a proxy server.

31. (Canceled)

32. (Currently Amended) A computer readable medium having stored thereon a data structure representing a Session Initiation Protocol (SIP) request, the data structure comprising:

a plurality of SIP headers comprising an echoed header including an address of a SIP node in a route for the SIP request; and

data representing a digital signature generated by signing a portion of the SIP headers with a session key, wherein the echoed header is one of a group consisting of a VIA header, a FROM header, a TO header, a RECORD-ROUTE header, a CALL-ID header, and a CSeq header, wherein the data representing the digital signature is appended to one of the SIP headers, wherein the plurality of SIP headers comprises a plurality of VIA headers and the digital signature is generated based on all VIA headers in the SIP headers except a topmost VIA header.

33. (Canceled)

34. (Previously Presented) A computer readable medium having stored thereon a data structure representing a Session Initiation Protocol (SIP) request, the data structure comprising:

a plurality of SIP headers comprising an echoed header including an address of a SIP node in a route for the SIP request, wherein the plurality of SIP headers comprises a plurality of VIA headers and the digital signature is generated based on all VIA headers in the SIP headers except a topmost VIA header of the VIA headers;

data representing a digital signature generated by signing a portion of the SIP headers with a session key, wherein the echoed header is one of a group consisting of a VIA header, a FROM header, a TO header, a RECORD-ROUTE header, a CALL-ID header, and a CSeq header.

35. (Original) The computer readable medium of claim 34, wherein the digital signature is generated based upon a URI portion of the RECORD-ROUTE header and a URI portion of the CONTACT header.

36. (Original) The computer readable medium of claim 32, wherein the digital signature comprises a first signature generated based upon at least a portion of a RECORD-ROUTE header and a second digital signature generated based upon at least a portion of the RECORD-ROUTE header and at least a portion of a CONTACT header of the SIP request.

37-41. (Canceled)